ABSTRAK

Dengan kemajuan teknologi informasi dan komunikasi saat ini menjadikan *Cybercrime* salah satu ancaman besar pada sistem komputer ataupun *device* lainnya yang terhubung dengan internet, berbagai macam cara telah dibuat untuk mengatasi ancaman ini salah satunya dengan sebuah sistem Honeypot. Honeypot merupakan salah satu paradigma baru dalam keamanan jaringan yang bertujuan untuk mendeteksi kegiatan yang mencurigakan, membuat jebakan untuk penyerang (*attacker*) serta mencatat aktivitas yang dilakukan penyerang, walaupun sistem Honeypot terbukti dapat menjadi solusi terhadap keamanan sebuah jaringan tetapi dalam pembacaan terhadap aktivitas *log* yang dihasilkan masih menjadi masalah. Maka dari itu dalam penelitian ini penulis mengusulkan metode Elasticsearch, Logstash, Kibana dan *Regular Expression* untuk dapat membantu dalam analisis maupun *monitoring* secara *realtime* pada sistem Honeypot, Pada proses parse data dengan *Regular Expression* Cowrie memiliki nilai akurasi pada *pattern* 1 sebesar 98.14 *percent* dan *pattern* 2 mendapat 93.90 *percent*. Sedangkan pada 12 data Dionaea pada *pattern* 1 dan 2 mendapat akurasi 100 *percent*.

Kata Kunci: Honeypot, *log* analisis, ELK Stack , IoT Honeypot*, visualisasi*, *Regular Expression*.